Assumption Busters Workshop – Defense in Depth

Background: the U.S. Federal Cyber Research Community is conducting a series of four workshops designed to examine key assumptions that underlie current security architectures in cyberspace. These "Assumption Busters" meetings are designed to create the environment for the development of novel solutions that are based on a fundamentally different understanding of the problem and creates a stronger basis for moving forward on well-founded assumptions.

In the next few months, we will assess the problem for each assumption as well as any potential weaknesses that transcend the four categories: defense-in-depth, trust anchors, data dispersion, and malicious actors.

Introduction: the first "Assumption Buster" workshop was held on 22 March 2011 in Arlington, Virginia to focus on the assumption that "defense in depth is a smart investment". Over 50 participants from academia, government, industry and the research community attended the day-long open discussion. This paper identifies key themes from participants (either in discussion or supporting one-page contributions) that support or challenge the assumption. It then identifies near- and long-term directions for further research and exploration.

Assumption: Defense in Depth (DiD) is a smart investment.

Bottom Line: While participants expressed serious concern about the concepts and the implementation of defense-in-depth (DiD) as a cyberspace security strategy, they also pointed to approaches that could lead to its improvement. While some argued that we should cast it out of our thinking, many argued that the concept should be reconsidered and modernized.

Ideas that Support the Assumption:

--There is an improved understanding of some of the underlying elements of DiD, such as our understanding of attack sequencing and activities. Strong work on insider threat is continuing. Understanding and modeling the physical systems and processes that are controlled by networked systems is typically easy to do. Application white listing, design of secure systems and applications, and security by isolation are approaches that work. However, a number of solutions have been identified but not implemented.

--DiD still works when managers align security policies and practices with how a system is actually used (vice how they wish they would be used); most successful DiD systems exhibit characteristics where: a) a critical function must be able to operate at several levels of penetration, b) sections of defenses that have fallen cannot be turned against the defender, and c) defensive capabilities must be mutually supportive.

--The real potential value of DiD is the slow decay of system effectiveness *until a defense or counterattack could be mounted*. It is unreasonable to expect that DiD will provide complete defense, but rather buys diagnosis and response time, and may allow a system user to "play hurt" (to draw upon a sports metaphor).

--As is increasingly recognized, security that is conceived when the system is conceived is the most effective. This includes the system purpose and the concept of operations as well as an adversary model and the consequences and effects of potential attacks. Who would want to cause the system to fail at its purpose? Planning for failure within a DiD strategy is also an important part of the planning process – users need to be deliberate in thinking about attacks and any potential solutions.

--DiD is capable of stopping or deterring adversaries with lesser capabilities.

Ideas that Challenge the Assumption:

--DiD implies a sense of direction, which may not apply in cyberspace. Layered defenses may be a more appropriate term given the temporal, spatial, and other dimensions of the operating environment. The rapidly growing and shifting use of mobile devices and platforms will exacerbate this conceptual understanding.

--One weakness of DiD is the lack of integration across different protection mechanisms. Cyber threats can emerge within many paths: the network, removable media, the supply chain, innocent or malicious insiders, or physical access. An effective defense against one may be of no use against another. But layering ineffective solutions will not create an effective defense.

--DiD may only be as good as its weakest layer. Encryption is great for point-to-point protection but it can also mask information that other layers are designed to identify and stop.

--Our cyber adversaries are diverse and creative, ranging from highly capable individual antagonists to advanced persistent threats. They purposely seek out countermeasures to DiD.

Areas for Further Research and Exploration:

--**The Need for More Rigorous Definitions:** Many are concerned that there is still a lack of rigorous definitions for cybersecurity, information security, network security and other terms that hinder progress, or that allow different interpretations that limit solutions. Moreover, not all in the security community agree on what a comprehensive DiD strategy contains. We also need to understand the definitions and relationships between reliability, resiliency, robustness, survivability, and security better. For example, robustness enables a system to function in the presence of errors and failures, survivability enables a system to maintain "mission" in the presence of attacks and failures, while resilience enables a system to maintain all critical functions in the presence of attacks and failures with necessary response and recovery capabilities.

--**Understanding the Adversaries:** Our cyber-adversaries are very creative, ranging from surprisingly capable individual antagonists to nation-state attacks. At the sophisticated end of the spectrum lies advanced persistent threats, which are embedded in cyber systems at all times, observing and waiting to act at a time of their convenience. What can we learn from their behavior from both an offensive and defensive perspective?

--**Human Factors in Cyberspace:** Human dimensions are as important as network and system dimensions in approaching cybersecurity. We need to better understand human understanding and risk valuation of activities in cyberspace, including security, and we need to plan architectures and systems for how people use them, not how we'd like them to be used.

--**Can We Layer Defenses?** Building on the layered defense concept as a modification of DiD, are there ways in which to rapidly expand or deepen the layers? Can we envision a 100- or 1000-layer deep defense with different gradient filters at every step of the way?

--**Need for New and Improved Analytic Methodologies**: a number of topics cry out for new assessment tools and methods: there is no general methodology to demonstrate, for example, that adding a capability improves security (or not). What metrics exist for DiD? How can we assess the differential costs to improve security by diminishing the occurrence, severity, or timing of a cyber attack? Can we create something that encourages users to want security beyond its economic valuation? How do we take defensive concepts to a viral level in cyberspace? Can we create a game that encourages that? We also need better modeling—of adversaries, ourselves, third-party participants—in order to understand potential attacks and their impact. Finally, what are potential "black swan" event(s) in cyberspace?

--**Areas for Improved Government-Industry Cooperation:** while government and industry roles do not overlap entirely, there are many areas of common concern. For example: the IPv6 standard requires new security protocols: industry is waiting for government to mandate while government is waiting for industry to invent solutions.

--**Need for Entirely New Paradigm(s):** those who wanted to eliminate the concept of DiD as a legacy concept pointed to areas as wide ranging as biodiversity and public health to game theory and economics as potential sources of replacement frameworks. We need to understand the implications of the much more transparent and open framework that is rapidly emerging.